THIRD-PARTY RISK MANAGEMENT

AKINGBADE AKINFENWA

TABLE OF CONTENTS

INTRODUCTION

Third party risk management refers to the management of reputational, financial and legal risks for the organization by third parties; that is to say: by entities outside the company. It is a structured, consistent and continuous process, which is developed through the use of different tools for the identification, evaluation, and measurement and reporting of events and incidents that affect the possibility of achieving the objectives by the organization to whom the advice is provided.

Sometimes also just referred to as TPRM, Third-Party Risk Management is a discipline around analysing and controlling risks associated with outsourcing third-party vendors or service providers. Third-party and vendor risk assessments is an exercise you can conduct to help your organization determine how much risk exposure you'd take on if you were to outsource a business process or entrust your data to a third party.

Third-Party Risk Management (TPRM) is a form of risk management that focuses on identifying and reducing risks associated with the use of third parties (suppliers, partners, contractors, or vendors of services). It is designed to give organizations an understanding of the third parties they use, how they use them, and what safeguards they have in place.

The scope and requirements of a third-party risk management program depend on the organization and can vary widely based on industry, regulatory guidance, and other factors. Even so, many of the TPRM best practices are universal and applicable to all companies or organizations.

There are turbulent times for organizations today, especially when it comes to Third Party Risk Management. How do organizations select and supervise third parties? There are many reasons why the company should pay attention to third party risk. The number of suppliers and other players that companies engage with is growing dramatically, along with the risks they pose. As markets expand and organizations seek to compete, increasing globalization is inevitable—that competition occurs in new markets. This involves working closely with third parties. Intermediaries represent the greatest bribery risk for companies. 75% of bribery schemes are executed through an agent or other third party. What's more, regulatory agencies view third parties as a direct extension of their organization. It is expected to protect against the risks that every business faces, including the increasingly complex web of its third parties.

The term third-party risk management is also known as vendor risk management (VRM), vendor management, supplier risk management, or supply chain risk management. However, TPRM is often viewed as the umbrella discipline encompassing all types of third parties and all types of risks. Third-party risk management helps the organization understand what the people or organizations with which it has relationships are doing, how they do it, and how those actions may affect its ability to achieve business objectives by keeping an eye on critical risk areas.

While third party risk is not a new concept, recent events and an increased reliance on outsourcing have brought the issue to the fore. An event like the current COVID-19 pandemic has impacted almost all companies and their third parties, regardless of size, location, or industry. A large number of the breaches that have occurred in recent months were caused by a third party. It must be remembered that most modern organizations rely on third parties to keep operations running smoothly. So when your third parties, vendors or suppliers are unable to deliver, there can be devastating and long-lasting impacts.

For example, many organizations that rely on a service provider to host a website or cloud application. If the provider fails, the website or app will also fail. The case of shipping goods is typical. If drivers from the shipping or inland company go on strike, it can delay expected delivery times and lead to cancellations and customer mistrust, which will negatively affect the bottom line and reputation of the organization.

Third-party Risk Management is the process of evaluation and control of reputational, financial and legal risks for the organization by third parties, outside the company. Third-party due diligence is the investigative process by which a third party is reviewed, to determine any potential concerns involving legal, financial , or reputational risk . It includes the review, monitoring and management of communication throughout the life cycle.

Too often, leadership failures over third-party management have damaged organizations, exposing them to massive fines and penalties. Even if the financial penalty can be managed, the reputational impact can have far-reaching consequences for many years.

Third Party Risk Management is a top concern for compliance leaders, but many organizations are still reaching agreement on how best to manage their third parties, limit risk and develop programs based on evaluations.

Outsourcing is a necessary component in running a modern business. Not only does it save a business money, but it's an easy way to tap into expertise an organization might not have back home. The downside is that without a proper third party risk management program in place, relying on third parties can leave your business vulnerable. It is therefore important to know some of the third-party risk management best practices that should be incorporated into a good TPRM program to mitigate risks such as:

EVALUATING SUPPLIERS

It is convenient to classify the suppliers, since not all of them are equally important, so it is essential to determine which third parties are most important. To improve efficiency in a TPRM program, providers can be segmented into levels of criticality, for example.

- Level 1: High risk, high criticality
- Level 2: Medium risk, medium criticality
- Level 3: Low risk, low criticality

Thus, in practice, organizations will focus their time and resources on Tier 1 providers first, as they require more stringent due diligence and evidence collection. Tier 1 providers are typically subject to the most in-depth assessments, often including on-site assessment validation. To classify providers by levels, the inherent risk of the third party can be used, which is based on whether certain information can be shared with the provider, as well as the impact caused by not providing a service. Contract value can be useful to help segment. Big budget vendors may be automatically targeted as a Tier 1 vendor due to high risk based on contract value alone.

AUTOMATION AND ANALYSIS

Efficiencies arise when operations are consistent and repeatable. There are a number of areas in the third-party risk management lifecycle where employing automation is ideal. For example:

- Incorporation of new suppliers. Automatically add supplier information to the general list using an intake form or through integration with contract management or other systems.
- Calculation of the inherent risk and staggering of suppliers. When admitting a new vendor, basic business context information must be collected to determine its inherent risk, which allows you to automatically prioritize the vendors that pose the highest risk.

- Activation of supplier performance reviews. Automation triggers can be configured to perform a vendor review every year, and if the vendor fails the review, trigger other types of actions. You can also plan a reassessment based on contract expiration dates and use the responses from the previous year's assessment so you don't start the vendor assessment from scratch.
- Scheduling and execution of reports. You can set up automated reports that run daily, weekly, or monthly and are automatically shared with the right person.

Every third-party risk management program is different, so repeatable processes that are ripe for automation should be reviewed. From there, key tasks can be automated. Over time, these small automations will be a robust set that saves time and money.

CONSIDER DIFFERENT RISK MANAGEMENT

When considering a third-party or vendor risk management program, many organizations immediately think of cybersecurity risks. But TPRM involves much more. It's a good idea to start small and focus on those risks that need to be prioritized. For example:

- reputational risks
- strategic risks
- financial risks
- operational risks
- Compliance risks
- ethical risks
- Business continuity risks

And many more. The important thing is to understand all relevant types of risk (and not just cybersecurity), which is imperative to building a world-class third-party risk management program. The third-party risk management life cycle will be synthesized in a future article.

COMMON TYPES OF THIRD-PARTY RISK

The risks faced when working with third parties are much the same as other business risks and they usually fall into three categories:

- **Financial and Reputational**: When an organization must pay fees or fines, the potential loss of income is also a result of the reputational hit that sometimes follows a data breach.
- **Legal and Regulatory:** Third parties can negatively impact your organization's compliance with legislation. For example, if you are working with a vendor or supplier who violates labour, environmental, data security, or other laws, you can also be found liable.
- **Operational**: A third party could disrupt your operations in any number of ways, whether it's not providing the service you are paying for or through a data breach or outage that affects your data.
- **Compliance Risk:** What's the chance that working with this third-party will result in compliance issues with governmental regulations? Financial and medical industries have to pay special attention to this risk, as the penalties can be severe.
- **Cybersecurity Risk:** Data breaches and cyberattacks have been all over the news, with 7 out of 10 business leaders reporting increased cybersecurity risks according to an Accenture study. Communications with suppliers is a popular entrypoint for cyberthreats, so apply your due diligence to this field.

What you need is a formalized program for identifying and mitigating these risks accordingly across all your vendors. Two factors you have to keep in mind are prioritization and continuous efforts.

Not all risks are created equal, so prioritize them. Group your suppliers into categories based on their risk levels and focus your efforts where they matter most. For instance, your cybersecurity service provider will take precedence over the store that supplies your office stationery.

Keep in mind that risk assessment is an ongoing process. New risks will always introduce themselves as you work with new contracts and suppliers, so don't make risk management a one-time consideration. Monitor your business network in real-time so that nothing slips by unnoticed.

In some cases, these risks can overlap. A data breach, for example, is a regulatory threat, but can also disrupt your operations if you rely on their product or service to carry out a business process. A third-party data breach can also cause financial and reputational damage to your company.

WHAT TO INQUIRE IF YOUR ORGANISATION TAKES THIRD

"No organization is an island unto itself, each organization is a part of a larger whole."

This reflection aptly describes the postmodern organization of the 21st century, but if the relationship with "the whole" is not managed properly, it can have catastrophic consequences for the organization.

According to OECD.org, with around 70% of international trade today involving global value chains, an organization's services, raw materials, parts and components cross borders numerous times.

Today an organization is not just ONE organization, but includes vendors, service providers, contractors, subcontractors, consultants, temporary workers, agents, brokers, intermediaries, and a wide variety of other organizations “relationships with third parties”.

The complexity grows even more when we talk about companies that develop their services digitally. These relations with third parties, they help organizations run optimally, but they also expand attack surfaces as malicious actors increasingly target vendors, who can become the weak link in this chain.

By establishing or sustaining the wrong business relationships, a company can face not only financial catastrophe but reputational catastrophe as well. In this context, organizations must identify and govern their relations with third parties with increasing awareness.

Here are the questions to be considered if your organisation truly takes third-party risk seriously;

- **Does your organization perform due diligence prior to contracting with third parties?** Correctly evaluating a potential supplier can prevent the inclusion of risks to your organization. Assessments of a provider's information security, operational security, and business resiliency practices, including a provider's reputational standing, should be conducted.

- **Does your organization have a detailed list of third parties?** William Thomson Kelvin already told us what is not measured cannot be improved, what is not improved always degrades. A basic step to manage relationships with third parties is to create an inventory of suppliers, in short we cannot manage what we do not see. Inventory must be carried out on a centralized platform, so that all internal teams can participate in the supplier management process and it can be automated. In addition, it is important to create a profile for each provider, detailing their business prospects, the industry they belong to, demographics, the type of data they access, etc.
- **Can you identify the risk of third-party technology?** It is appropriate that the provider's profile includes information about its relationship with third-party technology, that is, with fourth parties. This can help visualize potential attack paths in your organization and take proactive mitigation measures.
- **Do you select your suppliers based on their compliance with international security standards?** It is important that when choosing a provider to assess whether it complies with the security standards known in the industry and also to verify if it can demonstrate compliance with these standards.
- **Do you control the providers affected by cyberattacks?** Observing a vendor affected by a cyberattack can help find signs of an impending new security incident by looking at what your vendor's vulnerabilities were.
- **Do you analyse externally available data to assess potential threats?** Risk identification starts with proactive analysis of not only internal but also external threat sources such as criminal forums, dark web, hacking databases, threat feeds, business news, financial data, etc. All this Third Party Risk Management can be developed individually, or solutions can be found that unify all knowledge in a single platform, so that all risks are centralized and visible to the company IT VRM solutions support businesses that have to assess, monitor and manage their exposure to risks arising from the use of third parties providing IT products and services or having access to your information. We must emphasize that Security Scorecard is one of the most widely used platforms in terms of Third Party Risk Management.

HOW TO DESIGN A FUTURE-READY RISK MANAGEMENT PLAN

This plan is essential in the development of an organization to the extent that it quantifies and evaluates the risks exposed by the set of entities (third parties and providers) that have access to its networks or that handle confidential data on its behalf, a reality of interdependencies that leaves open a large surface area for potential cyberattacks. In other words, there are numerous vulnerabilities in vendors or providers that are used to gain access to the target environment in order to steal or compromise sensitive information.

The high-performing risk management functions of the future will be notable for their skills and capabilities that go beyond technology. The following five steps should be considered when designing and implementing a future-ready risk management plan.

- **UPDATE RISK GOVERNANCE MODEL:** This adoption requires changes to traditional risk management models, although not necessarily drastic changes. For example, business leaders will need a comprehensive and complete view of financial and non-financial risks so that the company can control individual customer moments and processes in the long term. Risk and compliance functions need to integrate with business functions to understand and help design the latest product and service innovations. Designing risk into products and services allows for automation of future monitoring, once the change is in production. They will need this commitment to manage and monitor real-time risk, predictive business models, and meaningful interactions with third parties. Another feature that has been updated is providing information and expectations to help the company monitor overall effectiveness.
- **MAKE SURE THE TEAN HAS THE RIGHT SKILLS:** New skills (both "soft" and "hard"), are needed for new risk management approaches. For example, companies will need people with the skills and knowledge to cover all topics (compliance, operational risk, resilience) to manage the customer process, and for specific new types of risks (cloud, cyber or blockchain). Having the right skills on the team at the right time to make specific changes will help identify new and emerging risks.
- **ENABLE PRODUCTS AND SERVICE MANAGEMENT CAPABILITY:** Incorporating risk controls into product development processes in real time requires companies to have technology to track customer actions, with automatic triggers on products and services that are designed with a set of

security rules. Risk to instantly adjust the features of such products (for example, price or terms and conditions). Risk management leaders should also collaborate with the business on the initial design of the product. The goal should be to identify a comprehensive set of customer attributes and behaviour that relate to the key considerations. These insights are necessary for banks to quickly launch, scale, and manage new products and services.

- **STRENGHTEN RESILIENCE:** Resiliency, cybersecurity, and privacy are critical considerations in meeting customer expectations for reliability and protecting brand reputation and information assets. This needs to be infused throughout the company, including third-party vendor operations, especially with critical vendors. Since preparation is essential for resilience, companies must run simulations in a variety of disruptive or crisis scenarios.
- **ADVANCED DATA INTELLIGENCE:** There is no doubt that risk functions will try to use data more efficiently and automate more processes in the future. To do this, they will need a robust platform that integrates with a broader ecosystem of corporate governance, risk, and compliance. These platforms can enable more automated risk monitoring and support stronger data models to improve business intelligence and decision making.

The need to build trust and engage consumers at critical moments is transforming the future of risk management across all financial services. As business models evolve in response to technology-driven disruptions and rising customer expectations, risk management functions must similarly transform their approach and capabilities.

While there are many moving parts , including technology, processes, people, and organizational and cultural factors, for risk management leaders to manage in this evolution, the primary goal of building trust with the most demanding customers should serve as a guide in the journey.

WHAT GIVES RISE TO THE INREASE OF THIRD-PARTY RISKS?

THE INCREASING DEPENDENCE OF ORGANISATION ON THIRD-PARTY SOFTWARES:

An example of this would be that many businesses use payroll, customer relationship management, and email marketing solutions that are readily available and don't require engineering anything in-house. But this also means organizations are putting more of their data into third-party applications and creating more risk.

ORGANISATIONS HAVE BECOME SO RELIANT ON NETWORK COLLABORATORS:

There are many collaborators that organizations may rely upon to get things done such as partners, suppliers, vendors, and contractors. Increased information sharing and collaboration have enlarged the attack surface for cyber intruders.

GUIDELINES FOR THE RISK MANAGEMENT OF THIRD-PARTY

When we talk about third parties we tend to think that they are only our suppliers, however, the spectrum is broadened by also contemplating contractors, business partners, commercial agents and all those who support the operation, provide services, distribute and sell our products or services.

Third parties have access to the organization's information and can process confidential or sensitive data, they are an important part of our organization's operation, however, they can also be an important source of risk since cybercriminals often look for through them reach your customers; That is why it is so important to know their security posture as well as to know what efforts and measures they take to strengthen it.

A competent plan to minimize risks to third parties should include the following strategies:

1) Evaluate annually, as a minimum, the risk of third parties in the Board of Directors. To do so, it is necessary to include this fundamental issue on the Board's agenda through the audit committee.
2) Categorize the suppliers according to the access they have to our systems and information, and define a continuity plan if any of those suppliers had a cybersecurity incident.

It is even possible to assess the level of severity of the security incident, if this could put the corporation in serious jeopardy and, therefore, if the relationship with that provider should be reassessed, a warning formally issued or, in the worst case, cases, suspend the relationship and even claim damages.

3) Define the security standards expected from each of the providers in terms of third-party risks (cybersecurity, information security, operational resilience, etc.) and specify in the contract that if these standards are not met they will be You can terminate the contract immediately and without further explanation. The level of expectations of the requested standards is communicated to them from the beginning and suppliers are expected to abide by these indications in a responsible manner.
4) Ensure that auditors and CIO communicate regularly with vendors and are asked to update documents and security assurances. Information Technology and the way content is consumed on the Internet is advancing at great speed and it is part of the responsibility of your corporation's providers that they can maintain that level of security at all times now and in the future.
5) Define a third-party assessment framework in which third-party risks are assessed before signing an agreement with them, in which the frequency of re-evaluation and the standards they must comply with are established. The evaluation processes and periods make it possible to continuously certify that third parties are capable of carrying out their function.

Therefore, as an organization we must establish guidelines, processes and practices for the risk management of our third parties and identify what the selection, evaluation and monitoring approach should be.

- **IDENTIFICATION:** Before identifying the risk, we must know who our third parties are. This may not be an easy task, since the management of third parties may be decentralized and each area may be managing them independently. Once the third parties have built it, it is necessary to establish which services, platforms or assets they have access to and assess whether their permission levels are adequate for the service they provide us.

- **PRIORITIZATION:** Not all suppliers represent the same level of risk for our organization, so it is time to carry out a risk analysis that allows the assessment of each one to be established. For this, there are technological tools that comprehensively present the level of exposure of your third party and automatically assign you a cybersecurity posture assessment.
- **MONITORING:** In some cases, we have chosen to carry out annual surveys and assessments, however, these are just a snapshot of the moment in which they are carried out, so it is important to complement this process with continuous monitoring that shows the security posture of our third party and how they behaves over time, knowing if its level of risk increases or decreases according to the actions carried out by the third party. It is increasingly necessary to assume a proactive stance towards third-party management and jointly develop strategies that allow the assurance of the supply chain, this becomes a win-win, whereby, helping our third parties to identify their risks becomes valuable. So that they can develop mitigation actions.
- **AUTOMATE THE PROCESS:** Carrying out the risk management of our third parties is a process that takes us a long time, is expensive and in most organizations we do it through spreadsheets, which becomes unsustainable, which is why to mature the process and optimize management activities should be automated as much as possible.
- **CONSISTENT INFORMATION:** When sending the evaluations to our third parties, we can find different types of responses, as well as different formats through which they present the supports, which makes it difficult to establish the real state of their cybersecurity, in addition, the analysis of the information requires time and important efforts that in the end may not lead to the objective of the activity, being immersed in paperwork, for which it is necessary to ensure the consistency of the information, standardizing practices and processes as much as possible.

HOW ORGANISATIONS RESPOND TO THIRD-PARTY RISK

Companies are also discovering that third-party failures can tarnish its reputation with important implications in costs and image, affecting the operation and, even, causing non-compliance with regulations of various kinds. It is clear that companies need a clear strategy to manage risks associated with third parties and even with fourth parties. Given a large number of areas involved in the selection and contracting process of third parties, such as Purchasing, Legal, Quality and Compliance, it is evident that developing and implementing a continuous and consistent strategy represents a great challenge for companies. Almost all fraud or risk events involving third parties include company employees who benefit from the operation, although negligence and lack of controls they can be decisive.

Third party risk management is a process of identifying, evaluating and managing risks arising from third parties. These can be suppliers, customers, vendors or any other person or entity outside the organization that has some type of contact with it.

Companies must continually evaluate and analyse their environment to deal with possible vulnerabilities, their most important areas will always be economic, contractual and security.

Forward-thinking businesses do not evaluate third parties on a case-by-case basis. Instead, they put standards, policies, and systems in place to proactively mitigate risk continuously.

At this time, many organizations have deployed vendor risk assessment questionnaires to understand what risk management processes a vendor has in place, how they approach data security, and whether they can reasonably trust them to handle consumer data properly. However, a vendor risk assessment questionnaire shouldn't be the only part of your third-party risk assessment.

The downside of these vendor risk assessment questionnaires is that they only offer a point-in-time snapshot of your vendors' data security measures. Additionally, they're a self-assessment, so you can't independently verify a vendor's answers.

To increase due diligence on your vendors, you may consider conducting your own audits, at least on key vendors. For instance, Microsoft has created its own Supplier Privacy & Assurance Standards to instruct its suppliers on data privacy and protection and ensure its suppliers are compliant with those requirements.

Meanwhile, Adobe has a similarly structured program for its vendors. Adobe utilizes a vendor risk assessment program called Guardrails, which includes a set of requirements to which third-party vendors that collect, store, transmit, process, or dispose of sensitive data must adhere to. The Guardrails Risk Assessment program evaluates each vendor's compliance to Adobe's Vendor Information Security Standard, providing a risk-based review of the vendor's security practices and enabling Adobe managers to make fact-based decisions concerning whether or not to enter into a relationship with that vendor.

MX, a software company that creates software for financial and fintech companies, conducts a risk assessment when initially starting a relationship with a vendor and on an annual basis to identify any issues that need to be remediated. As part of this risk assessment, the services provided by a third party are evaluated to determine the types of data that will be processed by the third party. The level of sensitivity of data determines the depth of the security review performed on the third party. Findings from each security review are discussed with and provided to the third party to remediate within an agreed-upon timeframe.

HOW TO ADDRESS THIRD-PARTY RISK

Third party management is extremely important to ensure that service providers deliver quality deliveries, meeting set goals, but also without risk. After all, outsourcing is about establishing a strategic partnership, where companies work for your company and often within your facility. This also includes the service providers themselves, who must ensure full compliance with the rules, regulations and procedures. Such a level of trust can open some operational and strategic gaps that, without proper attention, can cause serious problems. We talk about operational, reputational, financial, data security and compliance risks.

When it comes to third-party risk management, there isn't a one-size-fits-all approach. What makes sense for a large organization like Microsoft or Adobe almost certainly will not sense for a three-year-old consumer-focused start up. However, here is a set of foundational items businesses of all types should consider:

- **UPDATE DATA MAP TO INCLUDE THIRD-PARTY VENDORS:** The foundation for your third-party risk management program should include all consumer data your vendors have in a data map. A clear view of what data your vendors can access and how they are using it will help you put the right agreements in place and ask for the right compliance information from each of your vendors.
- **HAVE A FRAME WORK FOR ASSESING THIRD-PARTY RISK:** Instead of assessing vendors on a case-by-case basis, your organization should have a third-party risk assessment framework in place before you even begin researching vendors and know exactly what you expect from potential third-party service providers. As a general rule of thumb, the framework should generally be a high-level guide that details exactly how vendor risk management will be handled. This guide will help to provide steps for senior management in different lines of business to follow. Generally, the guide will outline day-to-day vendor risk management responsibilities in explicit detail, so that no step is overlooked. A good place to start with this is reviewing any past application vulnerability assessments you've done, and seeing where those vendors had issues. You should also consult your company's compliance policies and requirements to make sure your vendor is able to meet the standards your company has set for itself.

- **VENDOR RISK MANAGEMENT PROGRAM SHOULD BE BASED ON INDUSTRY POLICY:** You can use vendor assessment programs from established enterprises (e.g., Microsoft, Adobe) as a starting point for your own vendor assessment framework. For instance, Adobe's Vendor Assessment Program whitepaper lays out the types of security controls they assess for every third-party vendor that stores or processes company data. Below is a sample of the controls and some of these may make sense for your organization as well:
    - Assertion of Security Practices: Review of security certification attestation reports (SOC 2 Type II, ISO 27001) and internal security policies and standards.
    - User authentication: Password policies, access control processes, and support of multi-factor authentication.
    - Data Centre Security: Physical security controls in locations where company data is hosted
    - Vulnerability and Patch Management: Cadence of external/internal vulnerability assessments and pen tests as well as timelines for vulnerability remediation
    - End-point protection: Policies that cover end-point security
    - Data Encryption: Encryption of data in rest and transit

In developing a vendor assessment framework, you may also find it helpful to look at some of the industry-standard cybersecurity risk management methodologies such as:

- SOC 2
- ISO 27001
- Consensus Assessment Initiative Questionnaire
- NIST Risk Management Framework 2.0
- NIST 800-171
- VSA Questionnaire
- CIS Critical Security Controls.

You can extract thousands of potential questions from these frameworks and adapt them for your own vendor assessment questionnaire.

- **DEVELOP A STRUCTURED VENDOR ONBOARDING AND OFFBOARDING PROCESS:** Just as you have an onboarding process for new employees to make them aware of your corporate policies, it is important to develop a standardized onboarding process for your vendors. In your onboarding process, you'll want to make sure vendors understand your information security standards/policies and have agreed to adhere to those standards. For instance, if a vendor plans to have individuals conduct work on your behalf on their own personal devices, you'll need to communicate your "Bring Your Own Device" restrictions on what data the vendor can and cannot store on their devices.
- **CONSIDER SECURITY EVALUATIONS:** Security ratings allow you to monitor your vendors and their vendors' security ratings in real-time. If your organization uses many vendors, this will allow your organization to streamline the vendor assessment process, monitor for changes in security posture, and request remediation of key issues at high-risk vendors. Businesses such as BitSight do the work of evaluating vendors for you so you can ensure you're partnering with secure, high-quality organizations.
- **FRAMEWORK SHOULD BE USED:** When it comes to risk management and compliance, implementing something is better than nothing. It's common for compliance and data security programs to need updates, tweaks, additions, and adjustments as you find processes that aren't working, encounter new risks or become subject to new privacy requirements. So don't wait until your vendor security framework is perfect – deploy it now and commit to consistent review and improvement.
- **ENSURE SELECTION PROCESSES ARE IN PLACE:** When it comes time to make a selection, you should have a vendor vetting process in place. Having one of these processes is another critical step in ensuring that you make the right selection of a third-party vendor for your organization. That said, making the correct perceived selection should only be a starting process, rather than the end all be all. During this vetting process, you may want to consider points such as comparing certain vendors to relevant competitors, issuing requests for proposals (RFP), and completing due diligence tasks such as completing a risk assessment as dictated by your policies.

- **ESTABLISH AND PUT CONTRACTUAL STANDARDS IN PLACE:** While it is okay, to begin with, a general template for the contracts that you put in place with a third-party vendor, it should also be understood that there are no two contracts that will be exactly alike. Make sure to communicate to ensure both parties have an understanding of responsibilities before a contract begins. The contract should include steps such as how things need to be negotiated, and the approval process for how contract changes should be made, in addition to how they will be stored and approved.
- **KEEP UP WITH MADE PLANS:** Due diligence is just as necessary as the policies put in place surrounding third-party compliance risk management. Keep up with your due diligence on an ongoing, sometimes annual basis. The success that you have with your vendor will be in direct proportion to your ability to continue understanding any changes your vendor may have gone through. There are several steps that you may want to take in your due diligence process. First, you will want to review the vendor's financial statements when they are released. You'll also want to continue to request and evaluate your vendor's SOC reports. Overall, several annual assessments should be conducted and completed, including reviews of risk, performance, and information security.
- **DEFINE YOUR INTERNAL VENDOR RISK AUDIT PROCESS:** An internal audit process is going to be an essential component of your vendor risk assessment program. A final internal audit will be a wonderful last-review process for your vendor before an examiner arrives on-site. It's a much better idea to catch any mistakes present in your process before your examiner does. Overall, it will also help to mitigate the presence of any risks that are present in general.

In addition, most companies depend on third parties that provide them with supplies or some kind of service, so their exposure to risks is substantially increased. That is why the importance of the way in which risk management is carried out in the company is vital for its survival in a more than competitive market.

This type of relationship obviously brings with it a large number of opportunities for customer satisfaction and the diversity of products to offer, but it is necessary to establish security limits in the face of risks to third parties.

At this point, the figure of the stakeholders is important, the main ones affected by the activities of third parties.

These groups are essential when preparing strategic business planning, so they must be assured of an environment of trust that ensures strategic growth.

SW, today collaboration with third parties is the key to success, but also a source of risk that, if not managed, can have fatal consequences for the company.

To understand a little more about what this deals with, the main third parties that generate alliances with companies are suppliers, brokers, agents or consultants, among others.

To all this, the organizations are the first responsible for the management that they do of the third parties with which they have relations.

In this sense, we find six relevant components to reinforce exposure to risks to third parties, through the design and implementation of coherent functions that provide efficiency.

These are;

- **OVERSIGHT AND GOVERNANCE:** The leadership of the governance of the organization and its supervision is fundamental, and even more so if good practices are integrated into the internal functioning of the company. Thus, it is important to assign responsibilities, which usually fall on the information security or compliance functions. This varies as the risk management system matures. In addition, a government structure must be established, as the backbone for the supervision and reduction of the same. And here the stakeholders are also very important, which must be involved in risk management to achieve true success.
- **THIRD PARTY INVENTORY:** You have to know and make an inventory of all the third parties with whom you have a relationship, assigning them a classification and evaluation in order to manage them. Thus, identifying the person responsible for the relationship with the company will be key, since it will speed up the management and data collection necessary for the inventory much more. In addition, it is advisable to create categories to prioritize actions against third-party risk management. Finally, it goes without saying that this inventory must be updated in the face of possible changes or modifications by either party.

- **APPROACH AND RISK MODEL:** To establish a risk-based approach, a model must be developed that considers the context of the organization, determining the level of risk that it is willing to tolerate. They must establish a system for the identification, evaluation and response to risks of external origin, to strengthen and improve their strategies and be better equipped against possible negative impacts. In addition, as a positive consequence, a maximization of the potential as a company is obtained.
- **POLICIES AND STANDARDS:** Implementing policies and standards allows defining the purpose and the different stages of the framework for risk management, assigning roles and responsibilities to stakeholders. Here, the Steering Committee is primarily responsible for compliance with the established policies and standards, in order to promote accountability in the most important stakeholders. In other words, any organization needs to establish a series of procedures that generate standards and guidelines that allow the management of risks due to third parties. Without these factors, it is difficult for the model to work.
- **THIRD-PARTY RISK MANAGEMENT PROCESS:** Once the process for risk management has been designed, it must be carried out. In other words, it is useless to have a framework for risk management, if it is not finally put into practice. Thus, for the risk management process to be fully effective, it must be considered as a continuous life cycle and for each and every one of the relationships with third parties. With this process, third parties are evaluated and qualified based on their level of risk, in order to proceed with their monitoring.
- **TECHNOLOGY, AUTOMATION AND REPORTS:** How to automate risk management in organizations is based on the use of management software and technologies that help to avoid or mitigate risks. Thus, using this type of technology will favour the automation of processes, the analysis of information in real time and the generation of reports instantly , which allow decision-making to be dealt with more efficiently

- **ISO TOOLS SOFTWARES:** Assuming that technologies are the best tools to face any type of challenge is no longer so difficult. The ISOTools Software allows you to manage your suppliers and other third parties, by monitoring the processes identified in your organization. The information in real time, thanks to the fact that it is in the cloud and does not require installation, will ensure an experience that you will never want to end.

To deliver true value, a third-party risk management program must be accompanied by ongoing measurement of key operational performance indicators and confirmation, especially with high-risk third parties, so that they operate ethically and transparently.

Even when the relationship formalized with a third party is based on the trust and credentials of said entity, leading practices suggest implementing preventive and control actions that support risk management on an ongoing basis or even help detect situations of alarm in the event that the actions of the third party, as well as their reputation, suffer negative changes or deterioration during the course of the contractual relationship.

Also, companies need to improve business resilience by accurately understanding the role that third parties play in generating goods and services for their customers, ensuring that they are in compliance with the policies and procedures applicable to the business and its environment.

BENEFITS OF THIRD-PARTY RISK ASSESSMENT

There is no doubt that third party management is an important part of the business routine that deals with outsourced companies. However, does investing in these practices really benefit the operation? For many organizations, this is such a "common" process that there aren't even dedicated guidelines, parameters, and tools. However, whether for businesses with one or more outsourced activities, it is essential to develop this stage of their operation, in order to avoid losses and strengthen their business culture.

Third-party risk management is critical for making sure the companies you are associated with uphold relevant laws, regulations, and industry standards. Traditionally third-party management addresses risk arising from financial health, IT security or data protection. Yet compliance and reputational risk are also important. Consumers can be unforgiving when unfair practices at a third party come to light – and your company is likely to suffer the consequences.

The high demand for external risk assessment shows that business owners everywhere understand its importance. Benefits of undertaking an external risk assessment include:

- **Compliance:** Government regulations are a significant pain point for businesses with poor risk management. Not only do you risk heavy penalties and fines, but sanctions can result in a damaged reputation with your customers and partners.
- **Visibility:** Like most companies, you're likely to work with a large variety of vendors. It's easy to overlook a supplier, when analysing vendor-relationships, due to sheer volume or habit. Having a formal assessment system in place by a third party ensures a non-biased and complete look at every connection you have with business partners.
- **Risk Reduction:** Determining what the exact risk is for each vendor enables you to keep a standard across all vendors. Through this, you can negotiate contracts that will ensure all vendors meet company policies at scale, minimizing potential risks.

COMMON SHORTCOMINGS OF THIRD-PARTY RISK MANAGEMENT PROGRAM

Many companies fall short of thoroughly tracking their risks for several reasons. Most of the causes can be categorized into the following:

- **Poor Visibility Into Risk:** Using an outdated legacy approach can make it difficult to visualize risk across your vendors. A powerful integrated risk management platform that presents risk findings in cutting edge visuals is often needed to overcome this.
- **Health and Safety:** Likewise, check on the safety controls for both you and your partners. Any incidents in this field can cause significant damage which will affect your reputation and trust level in the market.
- **Financial Insurance:** Constant monitoring of the financial viability of your business and its partners in real-time is essential, and many companies don't have access to that kind of technology.
- **Social Responsibility:** Risks don't have to be financial in nature. Know your brand's environmental and social responsibilities and ensure that they are reflected in the suppliers you choose to work with. ESG is a key focus for vendors in 2022.
- **Cybersecurity Control Framework:** Having a framework with which to measure the cybersecurity posture of your vendors is essential. Attacks that impact third-parties will ultimately impact you as well.
- **Incidence Response:** Issues can come up unexpectedly. If you aren't ready for them ahead of time it could have a very large negative impact on your organization. Don't be caught without a fast response plan in place to ensure business continuity and minimal impact.

THIRD-PARTY INSURANCE POLICY

When talking about "third-party insurance policy," you are the first party, the insurance company is the second party, and another entity is the third party. So, although the term "third-party insurance policy" does not relate directly to third-party vendors, the concept is useful in the context of risk management.

This is because third-party insurance protects you against the claims by a third party for damage suffered when adverse events materialize. As an example, we can look at some consequences of cyber risk, and what is covered under first-party risk insurance versus third-party risk insurance.

What is first-party cyber risk coverage? In general, first-party cyber risk insurance would cover you against losses directly resulting from a cyberattack. For example, it would repay what you spend to restore your systems, to repair or replace hard or software, or possibly even loss of business from downtime.

Third-party risk insurance, on the other hand, might reimburse the cost of notifying your clients, perhaps cover court fees if a customer decides to sue you, or pay certain other damage claims. Because damage from a data breach can cost companies millions of dollars, handling cyber threat is an increasingly urgent focus of third-party risk management, particularly as cyber criminals often sneak in through the weakest security link in your supply chain – which may be your third-party. Managing cyber risk in your third-party network is critical to protecting your business.

THIRD-PARTY CYBER RISK MANAGEMENT

According to one 2021 report by the Ponemon Institute, 74 percent of organizations say they had experienced a cybersecurity breach in the previous 12 months because they gave “too much privileged access” to third parties.

Despite this worrying trend, 54 percent of companies also say they don’t assess the security practices of third parties before allowing access to sensitive or confidential data. Another 63 percent are in the dark about which third party has access to their networks, and what kind of permissions those parties have.

All these gaps leave organizations with large third-party networks vulnerable to all sorts of cyberattacks and security incidents. Your organization may be one of the 60 percent of companies that work with more than 1,000 third parties. These entities introduce significant cyber risk into your organization.

Are you aware of these enterprise risks? More importantly, are you prepared for them? This will pull back the curtain on third-party cyber risk and why you need a third-party cyber risk management program.

WHAT IS THIRD-PARTY CYBER RISK?

According to McKinsey, enterprise IT environments and third-party capabilities "are interpenetrated and indistinguishable." Simply put, third parties and expanding supply chains provide more footholds for cyber attackers to reach your organization.

For clever attackers, your supplier ecosystem is an attractive vector to exploit; a successful breach of even one third party gives the attacker a path to reach many organizations (that vendor's customers) in one shot. Such "supply chain attacks" have become increasingly common in recent years, as evidenced by events like SolarWinds, Kaseya, and Codecov.

Software-based supply chain attacks are on a particular upswing. Between 2020 and 2021, these supply chain attacks tripled, which prompted the May 2021 executive order from the Biden Administration to name such attacks as a key area of concern. Moreover, supply chain attacks are expected to contribute to cyber-criminal activity throughout 2022 and beyond.

Other factors can also increase your organization's third-party cyber risk. These include expanding supply chains, the adoption of cloud computing, the shift to remote work, and the increasing number of third-party vulnerabilities that threat actors can (and do) exploit. To protect your organization, you need third-party cyber risk management.

THIRD-PARTY CYBER SECURITY RISK MANAGEMENT

To minimize third-party cyber risk and its potential fallout, you need better visibility into third-party risks. This means you need to understand both the vendor and cyber threat environment by answering questions like:

- Who are our vendors?
- Which of our systems and data do they touch?
- How are they protecting our data?
- Who are the attackers who may compromise vendors' systems?
- How are they most likely to attack?

You also need a process to vet every third party's security and data privacy controls, and evaluate them against the third-party risk management regulations applicable to your organization.

Here's where third-party cyber risk management (TPCRM) comes in.

TPCRM is an organized way of analysing, monitoring, managing, and mitigating the various cyber risks associated with your third-party network. With TPCRM, you can also:

- Assess and track the state of third parties' cybersecurity and resilience;
- Automation of vendor security assessments and third-party due diligence to reach more vendors faster and quickly identify control and compliance gaps;
- Determine whether third parties are protecting your confidential and sensitive information;
- Develop security ratings and scorecards and based on each vendor's threat or risk level;
- Take informed risk-driven decisions to protect the organization and gain more confidence in vendor partnerships.

According to the Ponemon study, two-thirds of organizations said that the number of cybersecurity incidents involving third parties such as vendors is increasing. And yet, only 46 percent of that same group prioritize the management of outsourced relationship risks. If your company is similar to these firms, the disparity increases your risk of costly cyberattacks and data breaches, especially if:

- Third-party data and IT environments are insufficiently secure;
- Vendors use low-security methods to access your systems or data;
- Vendors don't encrypt your sensitive data and send it via unencrypted services like email.

These security gaps can compromise your networks, systems, applications, data, and even users. They may disrupt your day-to-day operations and affect your business continuity and sustainability. If a breach happens, you may lose business-critical data. That could damage your reputation, increase customer churn, harm your revenues, and ultimately prevent you from achieving your strategic goals.

Also, third-party security weaknesses could endanger your ability to meet compliance objectives – which can be a huge problem if you are required to comply with laws and regulations such as GDPR, HIPAA, PCI-DSS, or SOC2 to continue operating in your industry.

WHY SHOULD YOU USE A THIRD-PARTY CYBER SECURITY MANAGEMENT SERVICE?

You can protect your third-party ecosystem from cyberattacks by implementing strong security controls in-house. The other option is to contract with an external TPCRM service provider.

An experienced provider can provide clear oversight of the third-party cyber risks affecting your business. The provider can actively identify, prioritize, and remediate these risks posed by your suppliers, partners, and other supply chain relationships. It can also manage your critical information systems that third parties access or use, while creating a buffer between at-risk assets and cybercriminals.

The provider's specialists will examine and assess third-party cyber risk from every angle. They will also identify the third parties that can create long-term value for your business. Their solutions can also enable you to manage your entire third-party ecosystem across every relationship lifecycle.

If you lack a robust in-house third-party risk management program, an external service provider can help you:

- Stay on top of third-party risk with continuous monitoring, threat monitoring, and alert management;
- Streamline the TPCRM or TPRM program with advanced analytics, automated workflows, and machine learning;
- Design risk frameworks and carry out vendor risk assessments and vendor due diligence.

Outsourcing TPCRM does involve additional costs. The provider's reach and knowledge, however, can enable better risk decision-making and protect your organization from third-party risks. A good provider can strengthen your cyber defences and set up response plans in the event of a breach. All these benefits could outweigh the costs, so you might want to consider outsourcing your TPCRM program to an external provider.

IMPORTANCE OF VENDOR SCREENING OF THIRD-PARTY RISK ASSESSMENT

"McKinsey" suggests that organizations, led by their CIOs and CISOs, should form alliances with their third parties to minimize third-party cyber risk. So, to meet your risk mitigation requirements, your company should work with vendors, suppliers, and other third parties to sustain a united security front.

This doesn't mean blindly trusting every third party or expecting that their security goals are aligned with yours. If anything, you should invest more time and resources in conducting third-party risks assessments. Third-party due diligence is a crucial element of such assessments.

Due diligence means verifying every vendor's cybersecurity protocols and procedures. To help with such assessments, send due diligence questionnaires that include questions like:

- How do they identify an incident? Do they have an incident detection and response plan?
- How do they notify their customers (read: you) of security breaches?
- How do they follow-up after such incidents?

- Do they conduct penetration testing to find weaknesses in internal and external networks?
- How often and how quickly do they remediate any discovered issues?
- What data protection controls do they have in place?
- Do they conduct regular security testing? How often? Is the testing done in-house or by an impartial third party?
- Do they have a business continuity and disaster recovery plan?

You can, and should include questions about third parties' information security management, network management, and regulatory compliance.

Due diligence questionnaires are important to identify risks when welcoming and screening new vendors. They're also useful for assessing established partnerships and monitoring the security posture of existing vendors.

As your third-party ecosystem grows, due diligence questionnaires and vendor screening will all play a part in how you manage vendor risk and leverage third-party relationships to meet your business objectives.

ESSENTIAL STEPS FOR THIRD-PARTY RISK MANAGEMENT ASSESSSMENT

- **ONBOARDING:** When considering working with a third party it's important to do an initial risk assessment as part of the decision making process - prior to formally bringing a third party on-board. You can use external data to get a broader picture of the third party risk using, for example, cybersecurity ratings to gauge their security posture. This reduces the chance of unknowingly inheriting undesirable risk.
- **TIER:** Either as part of the initial risk assessment, ideally performed prior to onboarding, or as soon as the third party has been brought onboard there should be a tiering assessment performed. This assessment is performed internally and results in the third party being placed in a tier that dictates the type and frequency of assessments the third party will receive. Tier 1 or critical vendors are the highest tier. Some vendors may be at a tier that does not require regular assessments (for example the third parties that cut the grass). External data from, for example, security ratings providers could be used to adjust the tier level if necessary.
- **ASSESS:** Third parties in the upper tiers should have regular risk assessments performed. These should be based on the area of risk posed by the third-party. For example vendors who manufacture a component may have questions around employee, health, and safety while consulting firms may not. But all third parties would have questions regarding their security posture and financial viability. The frequency of these assessments would be based on the tier, with the highest tier having the most frequent assessments.
- **GENERATE FINDINGS:** When an assessment is returned there may be responses that are unsatisfactory or incomplete. Additionally any objective external data collected around the third parties financial or security posture should be evaluated at this time for any issues. Issues, or findings, can then be reverted back to the third party to respond.

- **FIND SOLUTIONS TO ISSUES:** There may be a period where an assessment goes back and forth, tasks are generated, issues are responded to, and evidence is provided if necessary. All communication should be captured for future reference. In the end, there may be some risks that are accepted.
- **REPORT RISK:** After identifying, analysing, and remediating the risk, report on it to the necessary parties. All stakeholders should be able to get the level of visibility they desire.
- **MONITORING:** As previously mentioned third parties should be continuously assessed, which ideally means monitoring for any changes in risk or performance. This can be done through more frequent assessments or external data feeds such as continuously updated cyber security ratings. Changes should automatically trigger an issue, assessment, and/or tier change. It is crucial to continuously monitor to ensure that all third parties are fulfilling their obligations and do not pose an undesirable risk to the organization.
- **RETIRERING:** All organizations should have a formal process to retire third parties and ensure all information that should not be stored is permanently deleted.

CONCLUSION

Working with a third party can introduce risk to your business. If they have access to sensitive data they could be a security risk, if they provide an essential component or service for your business they could introduce operational risk, and so on. Third party risk management enables organizations to monitor and assess the risk posed by third parties to identify where it exceeds the threshold set by the business. This allows organizations to make risk-informed decisions and reduce the risk posed by vendors to an acceptable level.

Third parties are an important key to the success of a business. Organizations of all sizes are becoming more and more reliant on third parties for their innovation, growth, and digital transformation.

But, a strong reliance on third parties can be risky. The risk posture of a third party is crucial to the risk posture, resilience, and reputation of a company using a third party. It can be very costly and difficult to deal with a third party incident, with consequences including regulatory actions, damage to reputation, and a loss of revenue. Third parties need to be carefully vetted with ongoing risk assessments to ensure that an organization is protected and secure.

Prior to now, vendor risk management has been time-consuming and error-prone, consisting of manual processes using emails, spreadsheets, and soloed vendor risk management tools. These processes and tools are simply inadequate, neither the tools nor the teams can keep up with the growing number of third parties. Common challenges faced by enterprises who haven't implemented modern or comprehensive solutions include:

- Manual Processes: Low efficiency with monitoring third parties and a longer amount of time to find and mitigate issues.
- Lack of scalability: Teams cannot keep pace with third party management when they are using a tool that will not scale, which can increase risk.
- Siloes: Too many siloes can create difficulty accessing risk information across the organization.
- Disconnected: No enterprise context makes it difficult to prioritize third party risks through the vendor lifecycle or when requirements change.

Strategy can be threatened when third parties and organizations aren't aligned on decisions and objectives. It is crucial to monitor third parties to make sure that strategic risk doesn't lead to a lack of compliance or eventual financial risk.

The reputation of a company can also hinge on the reputation of a third party with whom they do business. If a third party has an issue with reputation or a data breach, it can lower customer trust in a business that works with the third party.

Operations can sometimes hinge on third party applications and services, and there is always a risk that the third party can fall victim to a cyber-attack or a lapse in service that can lead to operational interruptions, a loss of data, or a privacy violation. If there are fourth parties involved the same concerns apply to them.

There can be issues with a product or service delivery from a third party, which can cause transactional issues within an organization.

Standards are slowly beginning to incorporate third party risk as a requirement for compliance, so risk tolerance for compliance should be extended to third-parties as well.

Regardless of whatever form data may take, there is a degree of risk that arises from allowing a third party to interact with data, including risk from unauthorized access, disruption, modification, recording, inspection, or destruction of information.

It is important to work with financially viable third parties to avoid disruptions to the supply chain. Additionally, third parties who are in financial trouble may not be as focused on security measures, leaving themselves open to unnecessary risk.

Further, the value of the tasks being executed by third-parties is increasing, increasing the impact of disruption or failure of third-party vendors.

Third-party risk is a feature on board agendas with CEO/board-level responsibility in many organizations especially those operating in regulated environments. Visits to third-party locations are becoming more common to gain assurance over third-party management.

REFERENCES

- Ivan Rodriguez C.P (2022). (AUDITCOOL SAS). (BOGOTA DC, COLOMBIA). https://www.google.com/search?q=apa+reference+style&client=firefox-b-d&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiP2NiC49X7AhWJuaQKHaRQAHsQ_AUoAXoECAEQAw&biw=1366&bih=643&dpr=1#imgrc=Fh70NNgyWEBjWM.
- Jingcong Zhao J.Z (2022). (hyperproof). (Seattle, Washington). https://hyperproof.io/resource/third-party-risk-management/
- RECIPROCITY (2022). https://reciprocity.com/resources/what-is-third-party-cyber-risk-management/
- SERVICENOW (2022). https://www.servicenow.com/products/governance-risk-and-compliance/what-is-third-party-risk-management.html
- Rocio Arrarte (2021). (Diligent). https://www-diligent-com.translate.goog/es/cinco-pasos-que-definen-buena-gestion-riesgos-terceros/?_x_tr_sl=es&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc
- ISOTools (2022). (ISOTools Excellence). https://www-isotools-org.translate.goog/2018/10/24/6-pasos-abordar-gestion-riesgos-terceros/?_x_tr_sl=es&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc
- RISKMETHODS (2022). https://www.riskmethods.net/resilient-enterprise/everything-about-third-party-risk-management